GrammaTech CodeSurfer

- Code analyzer tool with unique technology
  - Program Slicing
    - Highlights code relevant to understanding a particular issue
    - Does impact analysis
  - Pointer Analysis
    - Tracks loads and stores via pointers
    - Takes indirect function calls into account
- Typical uses
  - Reverse Engineering
  - Debugging
  - Safety/Security Auditing
  - Documentation

CodeSurfer (Cont'd)

- Automates common tasks
  - Trace the flow of data backward and forward through code
  - Display what variables a pointer can point to
  - Highlight code that affects selected statement(s) and/or variable(s)
  - Display the call graph, including calls through function pointers
  - Determine the impact of possible code changes
  - Extract detailed program information for documentation
- API for customization and batch processing
- Works on C
  - Beta version of CodeSurfer for C++ will be released 2003-Q4
- Users
  - NASA (MSFC), Mitre, MIT, Thales, Network Associates, others...

Buffer-Overrun Detector

- Statically finds buffer overruns
  - Plug-in to CodeSurfer
  - Current prototype developed with University of Wisconsin
- Technique based on Wagner's research at UC Berkeley
  - Examine program's structure
  - Build constraints for the ranges of buffer size and subscript values
  - Solve for ranges and flag unsafe cases
- Found:
  - 15 overruns in **`WU-FTPD`** that will be fixed in next release
  - 7 overruns in **`CLIPS`**